Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Review of the Emergency Alert System	)	EB Docket No. 04-296
	)	
	)	
	)	

Comments of VeriSign, Inc.

Anthony M. Rutkowski
Vice President for Regulatory Affairs
VeriSign Communications Services Div.
21355 Ridgetop Circle
Dulles VA 20166-6503
tel: +1 703.948.4305
mailto:trutkowski@verisign.com

Ashwin Puri
Product Manager, Wireless Services
487 East Middlefield Road
Mountain View 94043-4047
tel: +1 650.426.5193
mailto:apuri@verisign.com

Michael Aisenberg
Director, Government Relations
1666 K Street, N.W., Suite 410
Washington DC 20006-1227
tel: +1 202.973.6611
mailto:maisenberg@verisign.com

Brian Cute
Director, Government Relations
1666 K Street, N.W., Suite 410
Washington DC 20006-1227
tel: +1 202.973.6615
mailto:bcute@verisign.com

Filed: 24 January 2006

1. As the largest independent provider of intelligent infrastructure services spanning both the legacy PSTN and IP-enabled Next Generation Networks, including global messaging gateway services, VeriSign is an interested party in this proceeding in supporting and advancing "an accurate, wide-reaching public alert and warning system… critical to the public safety…to promote the safety of life and property through a robust communications system."[1] Such capabilities are essential to the effectuation of public safety and an array of other public interest and national policy objectives.

2. VeriSign urges that the Commission exercise its broad public safety authority and facilitate, as proposed in the *EAS NPRM* and discussed below, actions necessary to expedite availability of a more flexible, comprehensive global EAS system that includes interoperability of flexible EAS capabilities for public network infrastructure and services regardless of the underlying technology. We also note that the implementation of intelligent infrastructure such as messaging gateways, authentication, and authoritative interoperable directories are critical to bringing about many of the new capabilities sought in the *EAS NPRM*.

I. AN ACTIVE COMMISSION ROLE IN FACILITATING EAS CAPABILITIES AND EFFECTIVE COLLABORATION IN NATIONAL AND INTERNATIONAL EAS FORUMS IS ESSENTIAL

3. The Commission's brief review of ongoing EAS developments provides a snapshot into some of the forums, activities, and standards occurring domestically and worldwide. Indeed, the rather significant intergovernmental involvement and leadership of both the DHS National Communications System (NCS) in multiple ITU-T and IETF forums, as well as the U.S. Geological Survey in World Meteorological Organization (WMO) and OASIS to develop global Next Generation Network EAS capabilities deserve praise and emulation.[2] Both the emergence of new technologies, as well as

---

[1] See para. 61 *et seq.*, *First Report and Order and Further Notice of Proposed Rulemaking*, BC Docket No. 04-296, FCC 05-191, released 10 Nov 2005 [hereinafter referred to as *EAS NPRM*].

[2] *See, e.g.*, NCS Press Release, NCS Develops Pilot Emergency Notification Service, <http://www.ncs.gov/news/2003/press_release/030103.html>; USA, *Modifications to Interworking Framework for National Implementations of ETS*, ITU-T Doc. COM2-D47, Dec 2005; USGS, *RSS/XML and CAP Feeds*, <http://www.usgs.gov/homepage/rss_feeds.asp>; WMO, *Emergency*

greater interoperability among existing platforms, have compelled industry, governments worldwide, and diverse agencies in the U.S. to provide for the common safety of the public – particular during times of national emergency.[3]

4. The Commission need not become involved in specifying specific services and standards at this time. On the other hand, the FCC needs to be proactively involved in ongoing national and global intergovernmental EAS activities through expert Commission staff. This activity includes the establishment of open, interoperable EAS goals and capability requirements as a consensus emerges on appropriate public EAS services as part of a comprehensive homeland security suite.

II. INTEROPERABLE MESSAGING CAPABILITIES ARE INVALUABLE FOR EMERGENCY ALERTS TO BOTH GENERAL AND SELECTED PUBLIC POPULATIONS

5. The ability to reach the public across multiple public network infrastructures – especially the extremely large and growing base of CMRS devices – has been widely recognized. To achieve this capability, emergency messaging solutions must provide secure cross-carrier, cross-platform connectivity, which enables enterprises and government agencies to deliver text messages to customers or internal employees, regardless of carrier, location, and handset type. One- or two-way communication can be enabled through combinations of text, voice, instant messaging, or e-mail messages. Good emergency messaging solutions also provide web-based content management and reporting tools, giving government agencies the ability to send messages from a secure web page, plus the statistics, message-status, and two-way functionality needed to evaluate the effectiveness of messaging in real-time, across all channels.

6. VeriSign today has the ability to provide these capabilities across 150 countries through a robust global infrastructure. The challenge, however, arises in local systems that are then faced with broadcasting these messages across a large customer base. It is here that marketplace for premium messaging services is resulting in the

---

Response Activities (ERA), http://www.wmo.int/web/www/DPFSERA/EmergencyResp.html. See also, *Liaison on Emergency Telecommunications*, ITU-T SG2 TD 61, Dec 2005 for an overview of international emergency communications work organization, standards, and terminology.

[3] *See, e.g., Report on Emergency Alerting and Emergency Handling Initiatives*, GSM Association, Oct 2005.

development of high performance a robust and scalable alert engines capable of processing a large amounts of data and matching it against a large set of emergency system user preferences, including the delivery of personalized content to subscribers, anywhere, on any device, based on the preferences they set up. Especially important are Unicode features that support multiple language character sets.

7. The Commission should consider establishing an emergency alerts task force that joins both government and industry resources. Such an initiative should also include the leveraging of emerging commercial premium messaging services and platforms that allow providers to recoup the implementation costs for emergency alert capabilities.

III. AUTHORITATIVE DIRECTORIES AND COMMON INTEROPERABLE TECHNICAL CAPABILITIES ARE IMPORTANT FOR EAS, INCLUDING DISABILITY SUPPORT

8. All Emergency Alert Systems necessitate the simultaneous delivery of large numbers of messages to telecommunication users through all available media and applications. Advanced next generation directory-based capabilities allow messages to be sent to users in specific geographical users, with different language preferences, and tailored to people with disabilities. However, the implementation of these capabilities requires the availability of authoritative interoperable user directories containing location, language, or disability information. Such directories are also important for an array of important public safety, public interest, competitive, and commercial needs. See attached Appendix.

9. As discussed in VeriSign's comments in the Docket 05-271 broadband Internet consumer protection proceeding, as well as the Docket 04-295 broadband Internet CALEA proceeding, the continued availability and interoperability of authoritative directories is a requirement that is even more important today as it was twenty years ago when the Commission promulgated equivalent requirements in the *Computer III Decision*. The re-invention of the underlying *Computer III* public infrastructure objectives in a Next Generation Network world is a critical challenge facing the Commission.

* * * * *

Appendix

Authoritative Interoperable Directory Capabilities

Category	Requirement	General Description
basic capability	**CPNI Service Identifier**	Authenticated directory associated with all CPNI Service Identifier implementations
supplementary capability	**Number Portability**	Information relevant to whether the CPNI Service Identifier is subject to porting and ancillary porting related information
	Priority Access	Subscriber special priviliges during times of emergency or network congestion
	Roaming	Subscriber automatic or manual agreements related to roaming clearing
	Quality of Service	Subscriber quality of service preferences
	Directory Assistance	Subscriber restrictions on availability of information to the public
	CallerID	Subscriber preferences concerning the availability of CallerID information to calling parties
	Disability Assistance	Subscriber disabilities pertinent to communication services
	Language preference	Subscriber's language preference
	Personal emergency (E112/911)	Subscriber information relevant to public safety officials during a personal emergency
	Public emergency alerts	Subscriber public emergency alert preferences
	DoNotCall	Subscriber preferences concerning unwanted solicitation communications
	Payment Methods	Subscriber preferences concerning manner of payment for services
	Intercarrier Compensation	Subscriber information relevant to intercarrier compensation
	Service Specification	Subscribers preferred default service provider(s)
	Application Interworking	Information relevant to interworking among subscriber applications
	Profile Management	Subscriber profile information made available to the public or to specific users
	Presence	Subscriber preferences concerning location and status
	Availability	Identity preference expressions
	Location	Subscriber geolocation
	Push Management	Subscriber's preferences concerning receipt of information based on geolocation
	Digital Rights Management	Subscriber's preferences and authorizations for receipt and use of intellectual property
	Device Management	Information relevant to the use of subscriber terminal devices
	Authentication Credentials	Subscriber digital certificates or other authentication information
	Information verification level	Extent to which basic subscriber has been verified and when
protocol feature	**Authentication**	Authentication requirements for queries
	Auditing	Auditing of queries, including accounting mechanisms
	Multiple Syntax Support	Query syntaxes accepted
	Mutiple Language Support	Languages supported
	Extensibility and Localisation Mechanisms	Means by which additional directory schemas and modules can be created, discovered, and appended to queries